

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 09-282235

(43)Date of publication of application : 31.10.1997

(51)Int.Cl.

G06F 12/14

G06F 3/06

G06K 17/00

(21)Application number : 08-096900

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 18.04.1996

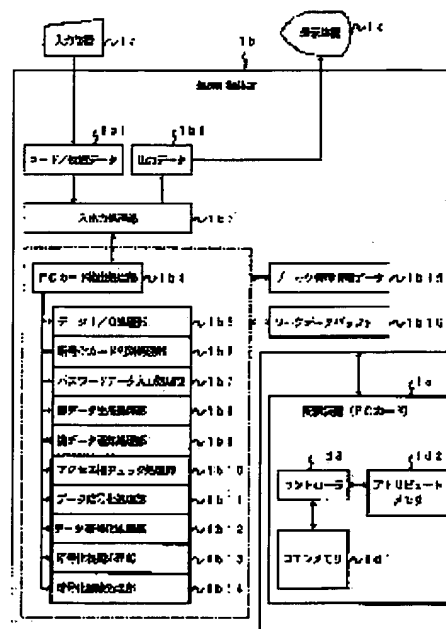
(72)Inventor : MIURA YOSHIYUKI

## (54) ACCESS CONTROL METHOD

### (57)Abstract:

**PROBLEM TO BE SOLVED:** To improve the security of a portable storage medium such as a PC card.

**SOLUTION:** When a ciphering request for using a non-ciphered PC card 1d as a cipher card is issued from a user, the user is urged to input a password to be used in key data generation for the ciphering and deciphering processings of the PC card 1d. Then, the password inputted from the user is stored in the PC card 1d, key data are generated by utilizing the data and the key data are presented to the user. Thereafter, based on the generated key data, the ciphering processing of the data already stored in the mounted PC card 1d and the processing of re-storing the ciphered data in the PC card 1d are performed. Thus, the ciphering is performed even to the PC card 1d in use in which the data are already stored.



## LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-282235

(43) 公開日 平成9年(1997)10月31日

(51) Int.Cl. <sup>9</sup>	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F 12/14	3 2 0		G 0 6 F 12/14	3 2 0 B
	3 0 4		3/06	3 0 4 H
G 0 6 K 17/00			G 0 6 K 17/00	E

審査請求 未請求 請求項の数 4 O L (全 12 頁)

(21) 出願番号 特願平8-96900

(22) 出願日 平成8年(1996)4月18日

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 三浦 佳之

東京都青梅市末広町2丁目9番地 株式会

社東芝青梅工場内

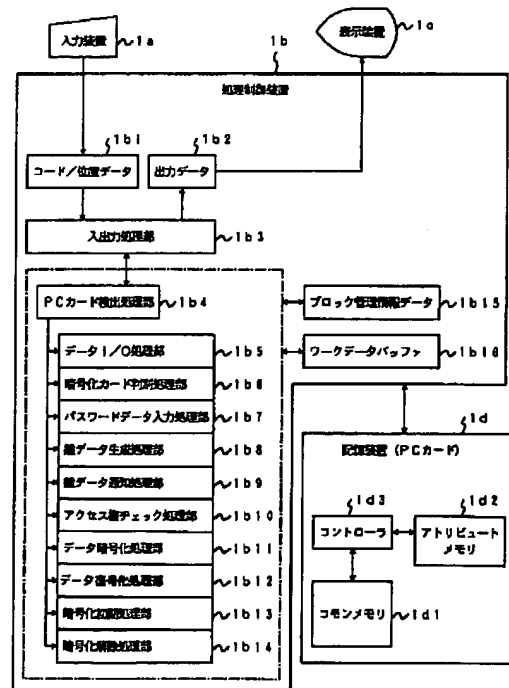
(74) 代理人 弁理士 鈴江 武彦 (外6名)

(54) 【発明の名称】 アクセス制御方法

(57) 【要約】

【課題】 P C カードなどの可搬型記憶媒体に対するセキュリティ性の向上を図る。

【解決手段】 暗号化されていない P C カード 1 d を暗号カードとして使用する暗号化要求がユーザから発行されると、P C カード 1 d の暗号化および復号化処理のためのキーデータ生成に用いるパスワードの入力がユーザに促される。そしてユーザから入力されたパスワードを P C カード 1 d に格納すると共に、そのデータを利用してキーデータを生成し、そのキーデータをユーザに提示する。この後、生成したキーデータに基づいて、装着された P C カード 1 d に既に格納されているデータの暗号化処理、およびその暗号化データを P C カード 1 d に再格納する処理が行われ、これによって、既にデータが格納されている使用中の P C カード 1 d に対してもその暗号化が行われる。



## 【特許請求の範囲】

【請求項 1】 可搬型記憶媒体が取り外し自在に装着される計算機システムで使用されるアクセス制御方法において、

前記計算機システムに装着された可搬型記憶媒体に対する暗号化要求に応じて、ユーザからの入力パスワードに基づいて前記可搬型記憶媒体に格納するデータを暗号化／復号化するためのキーデータを生成してそれをユーザに提示すると共に、前記入力パスワードを前記可搬型記憶媒体に格納し、

前記生成したキーデータに基づいて、前記装着された可搬型記憶媒体に既に格納されているデータを暗号化し、その暗号化データを前記可搬型記憶媒体に再格納し、前記暗号化データを格納する可搬型記憶媒体が前記計算機システムに装着されたとき、前記可搬型記憶媒体から読み出した入力パスワードから暗号化／復号化用キーデータを生成し、その生成した暗号化／復号化用キーデータとユーザから入力される暗号化／復号化用キーデータとの比較結果に基づいて前記可搬型記憶媒体に対するアクセス権の有無を判定し、

アクセス権を有すると判定されたとき、前記可搬型記憶媒体に対するデータ書き込み／読み出し要求に応じて、ライトデータの暗号化およびその暗号化データの書き込み、または暗号化データの読み出しおよびその復号化を行うことを特徴とするアクセス制御方法。

【請求項 2】 前記アクセス権を有すると判定されたとき、前記可搬型記憶媒体に対する暗号化解除要求に応じて、前記可搬型記憶媒体から前記入力パスワードを削除すると共に、前記暗号化されて格納されているデータを復号化して、前記可搬型記憶媒体に再格納することを特徴とする請求項 1 記載のアクセス制御方法。

【請求項 3】 可搬型記憶媒体が取り外し自在に装着される計算機システムで使用されるアクセス制御方法において、前記可搬型記憶媒体が前記計算機システムに装着されたとき、その装着された可搬型記憶媒体が暗号化媒体であるか否かを検出し、前記装着された可搬型記憶媒体が非暗号化媒体であるとき、ユーザからの暗号化要求に応じて、入力パスワードに基づいて前記可搬型記憶媒体に格納するデータを暗号化／復号化するためのキーデータを生成してそれをユーザに提示すると共に、前記入力パスワードを前記可搬型記憶媒体に格納し、前記生成したキーデータに基づいて、前記可搬型記憶媒体に既に格納されているデータを暗号化し、その暗号化データを前記可搬型記憶媒体に再格納し、前記装着された可搬型記憶媒体が暗号化媒体であるとき、前記可搬型記憶媒体から読み出した入力パスワードから暗号化／復号化用キーデータを生成し、その生成した暗号化／復号化用キーデータとユーザから入力される

暗号化／復号化用キーデータとの比較結果に基づいて前記可搬型記憶媒体に対するアクセス権の有無を判定し、アクセス権を有すると判定されたとき、前記可搬型記憶媒体に対するデータ書き込み／読み出し要求に応じて、ライトデータの暗号化およびその暗号化データの書き込み、または暗号化データの読み出しおよびその復号化を行うことを特徴とするアクセス制御方法。

【請求項 4】 前記アクセス権を有すると判定されたとき、前記可搬型記憶媒体に対する暗号化解除要求に応じて、前記可搬型記憶媒体から前記入力パスワードを削除すると共に、前記暗号化されて格納されているデータを復号化して、前記可搬型記憶媒体に再格納することを特徴とする請求項 3 記載のアクセス制御方法。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】この発明は、可搬型記憶媒体が取り外し自在に装着される計算機システムで使用されるアクセス制御方法に関する。

## 【0002】

【従来の技術】従来、半導体メモリを内蔵した PC カードやフロッピーディスクなどの可搬型記憶媒体に対するデータ書き込みにおいては、書き込みデータを変形させることなく、そのままの状態に記憶媒体に格納するという方式が採用されており、データを書き込んだユーザ以外の他のユーザでも簡単にそのデータに対してアクセスすることができた。なお、この方式におけるデータセキュリティ方式としては、ハードウェア的にはライトプロテクトスイッチによる書き込み禁止や、ソフトウェア的にはファイルの属性情報を変更することによる書き込み禁止ファイルや隠しファイルなどが知られている。

【0003】しかしながら、このようなセキュリティ方式を採用しても、PC カード内やフロッピーディスクのデータ構成は誰でも容易に解析および確認することができ、かつ、それらの属性も容易に変更することができるため、十分な秘匿性を得ることはできなかった。

【0004】また、セキュリティを考慮したデータの格納方式としては、PC カードなどの記憶媒体内にパスワードデータを格納し、アクセス時にパスワード入力を行うことにより、その記憶媒体に格納されているパスワードとの照合を行い、アクセス権をチェックした後、データライトおよびリードを行う方式が知られている。さらに、記憶するファイルまたはディレクトリ毎に暗号化処理を行うことにより他のユーザがアクセスしても有効なデータを取得することができないようにする方式もある。なお、この時に使用される暗号化用のキー（鍵）データは、それぞれファイルまたはディレクトリの属性情報として付加され、これを取得することにより、暗号化後のデータの復号化が実現される。

【0005】しかし、これらのセキュリティ方式においては、PC カードなどの記憶媒体内にパスワードまた

3

は暗号化／復号化用キーデータ自体を格納しているため、I/Oアクセス時には解析できないものの、記憶媒体内のデータを解析することにより、それらの取得を行うことができ、その後容易にデータをアクセスすることができる。つまり、単一レベルでの秘匿しか行っていないため、容易にそれを解除することができ、これも秘匿性の低いものであった。

【0006】

【発明が解決しようとする課題】 上述したように、半導体メモリを内蔵したPCカードや、フロッピーディスクなどの可搬型記憶媒体に対する従来のセキュリティ方式では、第三者が容易に属性を変更することができたり、パスワードや暗号化用のデータを解析し取得することができるため、個人単位で携帯する可搬型記憶媒体の個人情報情報を秘匿化するセキュリティ技術としては信頼性の低いものであった。

【0007】そこで、最近では、ファイルやディレクトリ単位ではなく、PCカードなどの記憶媒体単位でそこに書き込むデータを暗号化するセキュリティ方式が本出願人により提案されている（特願平8-42913号）。しかし、このセキュリティ方式は、PCカードフォーマット時に、そのPCカードに今後書き込むライトデータに対して暗号化処理を行うための設定をPCカードに対して行う方式であるため、使用中のPCカードについては、それを再フォーマットしない限り暗号化処理を行うことはできない。このため、既にデータが格納されているPCカードに対しては、そのデータを格納したままの状態では、そのPCカードを暗号化処理することはできない。また、暗号化処理されたPCカードの秘匿を解除する機能が用意されておらず、解除するためには、PCカードを再フォーマットしなければならないという問題があった。

【0008】この発明はこの様な点に鑑みてなされたものであり、使用中の可搬型記憶媒体に対してもその媒体単位で秘匿性の高い暗号化処理を容易に行うことができるアクセス制御方法を提供することを目的とする。

【0009】

【課題を解決するための手段】 この発明は、可搬型記憶媒体が取り外し自在に装着される計算機システムで使用されるアクセス制御方法において、前記計算機システムに装着された可搬型記憶媒体に対する暗号化要求に応じて、ユーザからの入力パスワードに基づいて前記可搬型記憶媒体に格納するデータを暗号化／復号化するためのキーデータを生成してそれをユーザに提示すると共に、前記入力パスワードを前記可搬型記憶媒体に格納し、前記生成したキーデータに基づいて、前記装着された可搬型記憶媒体に既に格納されているデータを暗号化し、その暗号化データを前記可搬型記憶媒体に再格納し、前記暗号化データを格納する可搬型記憶媒体が前記計算機システムに装着されたとき、前記可搬型記憶媒体から読み

4

出した入力パスワードから暗号化／復号化用キーデータを生成し、その生成した暗号化／復号化用キーデータとユーザから入力される暗号化／復号化用キーデータとの比較結果に基づいて前記可搬型記憶媒体に対するアクセス権の有無を判定し、アクセス権を有すると判定されたとき、前記可搬型記憶媒体に対するデータ書き込み／読み出し要求に応じて、ライトデータの暗号化およびその暗号化データの書き込み、または暗号化データの読み出しおよびその復号化を行うことを特徴とする。

【0010】このアクセス制御方法によれば、PCカードやフロッピーディスクなどの可搬型記憶媒体を暗号カードとして使用する暗号化要求がユーザから発行されると、可搬型記憶媒体の暗号化および復号化処理のためのキーデータ生成に用いるパスワードの入力がユーザに促される。そしてユーザから入力されたパスワードを可搬型記憶媒体に格納すると共に、そのデータを利用してキーデータを生成し、そのキーデータをユーザに提示する。このようにして、可搬型記憶媒体には、キーデータ生成に使用したパスワードだけが格納され、キーデータはアクセス制御方法を実現するためのI/O制御システムとして使用されるソフトウェア内部で保持管理される。この後、生成したキーデータに基づいて、装着された可搬型記憶媒体に既に格納されているデータの暗号化処理、およびその暗号化データを前記可搬型記憶媒体に再格納する処理が行われ、これによって、既にデータが格納されている使用中の可搬型記憶媒体に対してもその暗号化が行われる。

【0011】暗号化された可搬型記憶媒体が計算機システムに装着されたときは、アクセス権チェックが行われる。このアクセス権チェックでは、ユーザにパスワードではなく、キーデータを入力させ、それが、可搬型記憶媒体から読み出したパスワードから生成したキーデータと比較される。そして、アクセス権を有すると判定された場合には、データ書き込み／読み出し要求に応じてライトデータの暗号化およびその暗号化データの書き込み、または暗号化データの読み出しおよびその復号化を行う。

【0012】したがって、使用中の可搬型記憶媒体に対してもその媒体単位で秘匿性の高い暗号化処理を容易に行うことができる。また、記憶媒体には実際にデータ暗号化および復号化の際に使用されるキーデータを格納しておくのではなく、あくまでもそのキーデータを生成するための元となるパスワードのみが格納されているので、第三者が記憶媒体内のデータを単純に解析しただけでは秘匿を解くことはできない。よって、個人単位で携帯され、且つ計算機システムに着脱自在に装着して使用されるという特徴を持つ可搬型記憶媒体のセキュリティ保持に適したアクセス制御を実現できる。

【0013】

【発明の実施の形態】 以下、図面を参照してこの発明の

実施形態を説明する。図1には、この発明の一実施形態に係るアクセス制御方法が適用される計算機システムとそのシステムで実行されるプログラムの機能構成が示されている。ここでは、計算機システムに取り外し自在に装着可能な可搬型記憶媒体として、半導体メモリを搭載したPCカードを例にとって説明する。

【0014】この計算機システムは、キーボードやマウスあるいはペンやトラックボールなどからなる入力装置1a、および表示装置1cを有する計算機本体を備えており、この計算機本体にはそれが電源オンの状態であってもPCカード1dの装着、取り外しを行うことができる。

【0015】処理制御装置1bは、PCカード1dの計算機システム本体との挿抜判別、PCカード1dに対するデータ秘匿化の設定および設定解除、また、計算機システム本体からリクエストされたI/Oリクエストを判別し、データ暗号化および復号化処理を介してのPCカード1dへのデータI/O制御、また、これらの処理に応じた入力装置1aおよび表示装置1cを介しての入出力制御を行うものであり、その機能は、計算機システム本体内のCPUによって実行されるソフトウェアであるPCカードドライバを利用して実現されている。

【0016】この処理制御装置1bは、入力装置1aより入力されたコード/位置データ1b1と表示装置1cに出力される文字データやグラフィックデータなどの出力データ1b2を処理する入出力処理部1b3と、計算機システム本体に対するPCカード1dの挿抜の検出、およびPCカードの種類の判別を行うPCカード検出処理部1b4と、PCカード1dに対するI/Oリクエストを判別し、PCカード1dへのデータI/O処理を行うデータI/O処理部1b5と、PCカード検出処理部1b4により検出、判別されたPCカードが暗号化されたPCカードであるか否かを判別する暗号化カード判別処理部1b6と、暗号化されていないPCカード1dに対して暗号化/非暗号化の設定の選択および、暗号化する際の鍵データ(キーデータ)生成に使用するパスワードデータの入力およびPCカード1dへの格納を行うパスワード入力処理部1b7と、パスワード入力処理部1b7により入力、格納されたパスワードデータより、データ暗号化/復号化用のキーデータ生成を行うキーデータ生成処理部1b8と、キーデータ生成処理部1b8により生成されたキーデータをユーザに通知するキーデータ通知処理部1b9と、暗号化されているPCカード1dに対するアクセス権をチェックするためにキーデータの入力とそのデータの判別を行うアクセス権チェック処理部1b10と、暗号化されているPCカード1dに対してデータの書き込みを行う場合に、対象データを暗号化するデータ暗号化処理部1b11と、暗号化されているPCカード1dに対してデータの読み込みを行う場合に、対象データを復号化するデータ復号化処理部1b1

2と、計算機システム本体に正規のPCカード1dが装着され、そのPCカード1dに対して暗号化が設定された場合に、データI/O処理部1b5とデータ暗号化処理部1b11により既にPCカード1d内に格納されているデータの暗号化を行う暗号化初期処理部1b13と、計算機システム本体に正規のPCカード1dが装着され、PCカード1dに対して暗号化の設定が解除された場合に、データI/O処理部1b5とデータ復号処理部1b12により既にカード内に格納されているデータの復号化およびパスワードデータの削除を行う暗号化解除処理部1b14と、PCカード内に格納するデータを管理するためのブロック管理情報データ1b15と、各処理部にて使用される変数の格納やバッファとして使用されるワークデータバッファ1b16とから構成される。

【0017】また、PCカード1dは、計算機システム本体からのデータI/Oコントロール処理信号に応じてコモンメモリ1d1やアトリビュートメモリ1d2へのデータリード/ライト制御を行うコントローラ1d3と、このコントローラ1d3を介して計算機システム本体から送信されるデータを格納するコモンメモリ1d1と、PCカード1dの属性情報が格納されているアトリビュートメモリ1d2とにより構成される。なお、これらのメモリは、フラッシュEEPROMなどの不揮発性メモリを使用して構成される。

【0018】図2は、ブロック管理情報データ1b15の構成図である。PCカード1dのデータライトは、ハードディスク装置やフロッピーディスク装置同様、ブロック(セクタ)単位でのデータI/O制御によって行われるため、ブロック管理情報データ1b15は、図示のように、PCカード内の総ブロック数データ2aと、使用不能となった不要ブロックを管理するための不良ブロック数データ2bと、不良ブロックとなったブロックNo. 1~Nデータ2cと、不良になったブロックの代替先であるスペアブロックのスペアブロック数データ2dと、スペアブロックの代替ブロック数であるスペアブロック登録数データ2eと、スペアブロックNo. 1~Nデータ2fを備えて構成する。

【0019】図3は、アトリビュートメモリ1d2の構成図である。アトリビュートメモリには、PCカードサイズ3aと、スペアブロック数3bと、製造メーカー名3cと、リリースバージョン3dと、パスワードデータ3dなどのカード属性情報が格納されている。

【0020】以降、PCカードドライバを利用して実行されるPCカード1dに対するアクセス制御の手順を説明する。まず、アクセス制御処理の基本的な流れについて説明する。

【0021】PCカード1dの装着時には、それが暗号化カードであるか否かが調べられ、暗号化カードでない場合には、PCカード1dに対して暗号化処理を施すか

否かをユーザに選択させ、暗号化する場合に、その暗号化および復号化処理のための暗号化／復号化用キーデータを生成に用いるパスワードデータをユーザに入力させる。そして入力されたパスワードデータをPCカード1d内に格納すると共に、そのデータを利用して暗号化／復号化用キーデータを生成し、そのキーデータをユーザにアナウンスする。そして、既に格納されているデータの暗号化、およびその暗号化データの再格納が行われる。装着されたカードが暗号化カードであった場合には、ユーザに暗号化／復号化用キーデータを入力させ、PCカード1dへのアクセス権をチェックする。

【0022】具体的には、以下のステップを利用してアクセス制御が行われる。

(1) ユーザに対して入力や確認を促す入出力ステップ。

(2) PCカードと計算機システム本体との着脱状態や正規PCカードの検出および判別を行うPCカード検出ステップ。

【0023】(3) PCカードに対するデータI/Oリクエストを判別し、リクエストに対応するデータI/O処理を行うデータI/Oステップ。

(4) カード内データより暗号化されているカードか否かチェックし、その結果を入出力ステップによりユーザにアナウンスする暗号化カードチェックステップ。

【0024】(5) 暗号化カードチェックステップによりPCカードが暗号化されていないと判別された場合に、入出力ステップによりPCカードを暗号化するか否かの選択をユーザに促し、暗号化が選択された場合には暗号化／復号化用のキーデータの元となるデータの入力を促し、その結果ユーザが入力したデータをPCカード内に記憶するパスワード入力ステップ。

【0025】(6) パスワード入力ステップにより入力し記憶されたパスワードデータを元に、実際にデータの暗号化／復号化時に使用される暗号化／復号化用のキーデータを生成するキーデータ生成ステップ。

【0026】(7) キーデータ生成ステップにより生成されたキーデータを、入出力ステップによりユーザにアナウンスするキーデータ通知ステップ。

(8) 暗号化カードチェックステップによりPCカードが暗号化されていると判別された場合に、入出力ステップによりデータ暗号化／復号化用のキーデータの入力をユーザに促し、そのデータがPCカード内に記憶されるパスワードデータを元にキーデータ生成ステップにより生成されたデータを比較することにより、PCカードに対するアクセス権を判別するアクセス権チェックステップ。

【0027】(9) アクセス権チェックステップによりPCカードに対するアクセス権を取得した場合のPCカードへのデータ書き込みに対して、キーデータ生成ステップによりデータ暗号化／復号化用キーデータを生成

し、そのキーデータを元にデータを暗号化しPCカード内に格納するデータ暗号化ステップ。

【0028】(10) アクセス権チェックステップによりPCカードに対するアクセス権を取得した場合のPCカードのデータ読み出しに対して、キーデータ生成ステップによりデータ暗号化／復号化キーデータを生成し、そのキーデータを元にデータを復号化した結果をI/Oリクエストに渡すデータ復号化ステップ。

【0029】(11) 暗号化カードチェックステップによりPCカードが暗号化されていないと判別された場合に、PCカード内のデータの有無を判別し、パスワード入力ステップ、キーデータ生成ステップおよび、データ暗号化ステップにより、PCカード内に格納されたパスワードデータを元にデータ暗号化／復号化用のキーデータを生成し、このキーデータを元にPCカード内のデータを暗号化する暗号化初期処理ステップ。

【0030】(12) 暗号化カードチェックステップによりPCカードが暗号化されていると判別され、アクセス権チェックステップによりPCカードへのアクセス権を取得した場合に、入出力ステップによりPCカードの暗号化を解除するか否かの判別をユーザに促し、その結果ユーザが解除を選択した場合に、PCカード内に格納されているパスワードデータを削除し、暗号化されたデータを復号化する暗号化解除ステップ。

【0031】次に、図4のフローチャートを参照して、PCカードアクセス制御処理におけるメイン処理の流れを説明する。PCカード1dのアクセス制御は、計算機システム本体のメインメモリ（またはEMSメモリ）に常駐するPCカードデバイスドライバによって実行されるものであり、このPCカードデバイスドライバは、計算機システム本体を起動した際にメインメモリ（またはEMSメモリ）内への常駐や、PCカードに対するI/Oポートアドレスの割り当て、あるいはPCカードスロットのディスクデバイスへの割り当てなどの初期化処理を行い、計算機システム本体に処理を戻す（ステップ4a～4c）。これにより、PCカードデバイスドライバは、割り当てられたディスクデバイスに対応するPCカードの装着待ち状態となる。

【0032】計算機システム本体のPCカードスロットにPCカード1dが装着されると、計算機システム本体は、そのPCカード1dからのPCカード装着信号を検出し、PCカードデバイスドライバをコールする。

【0033】PCカードデバイスドライバは、計算機システム本体からのアトリビュートメモリセレクト信号を受け取り、PCカード検出処理部1b4にて、PCカード内のアトリビュートメモリ1d2のデータをワークメモリデータバッファ1b16内に取り込み、装着されたPCカードが本デバイスドライバが認識可能なPCカードであるか否かを判別する（ステップ4d、4e）。

【0034】この結果、本デバイスドライバが認識不可

能なPCカードと判別した場合は、入出力処理部1b3を介して、ユーザに、正規でないまたはフォーマットされていないのPCカードであることをアナウンスし、計算機システム本体に処理を戻す(ステップ4f~4h)。

【0035】また、本デバイスドライバが認識可能なPCカードと判別した場合は、暗号化カード判別処理部1b6にて、取得したアトリビュートデータ内のパスワードデータ3e領域内のデータをチェックし、暗号化処理が設定されているPCカードであるか否かを判別する(ステップ4i)。この結果、暗号化処理が設定されていないPCカードと判別された場合、暗号化カード判別処理部1b6は、入出力処理部1b3を介してユーザに、暗号化されていないPCカードであることと、そのPCカードに暗号化処理を設定するか否かの選択をアナウンス表示する(ステップ4j)。

【0036】もしユーザが、暗号化設定を選択した場合には、PCカード暗号化設定処理を行った後計算機システム本体に処理を戻し、設定しない方を選択した場合には、そのまま計算機システム本体に処理を戻す(ステップ4k~4h)。PCカード暗号化設定処理の詳細は図5を参照して後述する。

【0037】また、暗号化カード判別処理部1b6にて既に暗号化処理が設定されているPCカードと判別された場合には、そのPCカードに対するアクセス権を取得するために、アクセス権チェック処理部1b10にて、入出力処理部1b3を介してユーザに、暗号化処理が設定されたPCカードであることと、暗号化/復号化処理に使用されるキーデータの inputs を促す(ステップ4o)。そして、アトリビュートメモリより取得したデータ内のパスワードデータを元に生成したキーデータと、ユーザが入力したキーデータを比較する(ステップ4p)。その結果、両者のキーデータが一致しない場合には、入出力処理部1b3を介して、アクセス権が所得できないことをエラーとして表示した後、処理を計算機システム本体に戻す(ステップ4q~4s)。また、両者のキーデータが一致した場合には、入出力処理部1b3を介してユーザに、暗号化処理が設定されたPCカードであることと、そのPCカードの暗号化処理設定を解除するか否かの選択をアナウンス表示する(ステップ4t)。

【0038】もしユーザが暗号化設定の解除を選択した場合には、PCカード暗号化設定解除処理を行った後計算機システム本体に処理を戻し、設定解除しない方を選択した場合には、そのまま計算機システムに処理を戻す(ステップ4u~4x)。PCカード暗号化設定解除処理の詳細は、図6を参照して後述する。

【0039】また、計算機システム本体の入力装置よりPCカードに対応するディスクデバイスに対して、データライトあるいはデータリードなどのI/Oリクエスト

コマンドが入力された場合、データI/O処理にてPCカードの確認とデータI/O処理を行い、ステータス値をセットした後、計算機システム本体のデータI/Oコマンドに処理を戻す(ステップ4y~4a')。データI/O処理の詳細は、図7のフローチャートを参照して後述する。

【0040】次に、上述したPCカード暗号化設定処理、PCカード暗号化設定解除処理およびデータI/O処理の流れについて説明する。

10 (PCカード暗号化設定処理) まず、PCカード暗号化設定処理を図5のフローチャートを参照して説明する。

【0041】本デバイスドライバのメイン処理より本処理がコールされると、パスワード入力処理部1b7にて、入出力処理部1b3を介してユーザにデータ暗号化/復号化処理に使用されるキーデータを生成するためのパスワードデータの inputs を促す(ステップ5a)。ここで入力されたパスワードデータは、PCカード内のアトリビュートメモリ1d2内のパスワードデータ3e領域に格納される(ステップ5b)。

20 【0042】そして、このパスワードデータを元に、キーデータ生成処理部1b8にて、実際にデータ暗号化/復号化で使用されるキーデータを生成し、キーデータ通知処理部1b9にて、ユーザに生成されたキーデータをアナウンスする(ステップ5c、5d)。

30 【0043】また、PCカード内の既に格納されているデータに対しても暗号化を行うため、暗号化初期処理部1b13にて、PCカード内のブロック管理情報データを取得し、その情報に基づいてPCカード内のデータを取得し、データI/O処理部1b5内の暗号化処理を経由したデータライト処理を介してデータを暗号化して、その暗号化データを同一格納位置に再度格納した後、メイン処理に処理を戻す(ステップ5e~5g)。

【0044】(PCカード暗号化設定解除処理) 次に、PCカード暗号化設定解除処理を図6のフローチャートを参照して説明する。

40 【0045】本デバイスドライバのメイン処理より本処理がコールされると、暗号化解除処理部1b14にて、PCカード内の前記アトリビュートメモリ1d2データ内のパスワードデータ3e領域内のデータを削除する(ステップ6a)。なお、この時点でPCカード内に格納されていたパスワードデータは削除するが、本処理がコールされる前にメイン処理で取得したキーデータはメモリ内に保持される。

50 【0046】そして、PCカード内に既に格納されているデータに対しても暗号化を解除するために、PCカード内のブロック管理情報データを取得し、その情報とキーデータに基づいて、データI/O処理部1b5内の復号化処理を経由したデータリード処理を介して暗号化されたデータを元に戻した後、暗号化処理を経由しないデータライト処理を介して、再度データを同一位置に格納

11

する(ステップ6b~6c)。以上の処理を行った後、処理をメイン処理に戻す(ステップ6d)。

データI/O処理

(データI/O処理)次に、前述のデータI/O処理を図7のフローチャートを参照して説明する。なお、ここではデータI/O処理のうち、本発明に直接関係するデータライトおよびデータリード処理についてのみ説明する。

【0047】本デバイスドライバのメイン処理または、PCカード暗号化設定処理やPCカード暗号化設定解除処理より本処理がコールされると、データI/O処理部1b5にて、PCカードがデータI/O処理が可能な状態であるかを再度PCカード内のアトリビュートメモリ内のデータを取得して確認する(ステップ7a)。その結果、PCカードが認識可能なカードでなかったり、未装着であった場合には、入出力処理部1b3を介してその旨をユーザにアナウンスし、処理をメイン処理に戻す(ステップ7b、7c)。

【0048】PCカードがデータI/O処理可能状態であった場合には、コール時に受け取ったデータI/Oリクエストの内容より、各処理に分岐して処理が行われる。データI/Oリクエストがデータライトである場合、PCカード内のアトリビュートメモリ1d2内のパスワードデータ3eまたはメモリ内にキーデータが存在するかを判別し、存在する場合にはキーデータを使用してデータを暗号化し(存在しない場合には直接)、コントローラ1d3、アトリビュートメモリ内データおよびブロック管理情報データを介してコモンメモリ1d1にデータを格納し、ステータス値をセットした後、メイン処理に処理を戻す(ステップ7d~7h)。

【0049】また、データI/Oリクエストがデータリードである場合は、コントローラ1d3、アトリビュートメモリ内データおよびブロック管理情報データを介してコモンメモリ1d1のデータを取得し、PCカード内のアトリビュートメモリ1d2内のパスワード3eまたはメモリ内にキーデータが存在するかを判別し、存在する場合にはキーデータを使用してデータを復号化(存在しない場合には直接)し、ステータス値をセットした後、メイン処理に処理を戻す(ステップ7i~7m)。

【0050】以上のように、この実施形態においては、PCカード1dを暗号カードとして使用する暗号化要求がユーザから発行されると、PCカード1dの暗号化および復号化処理のためのキーデータ生成に用いるパスワードの入力がユーザに促される。そしてユーザから入力されたパスワードをPCカード1dに格納すると共に、そのデータを利用してキーデータを生成し、そのキーデータをユーザに提示する。このようにして、PCカード1dには、キーデータ生成に使用したパスワードだけが格納され、キーデータはデバイスドライバ内部で保持管理される。この後、生成したキーデータに基づいて、装

12

着されたPCカード1dに既に格納されているデータの暗号化処理、およびその暗号化データをPCカード1dに再格納する処理が行われ、これによって、既にデータが格納されている使用中のPCカード1dに対してもその暗号化が行われる。

【0051】また、暗号化されたPCカード1dが計算機システムに装着されたときは、アクセス権チェックが行われる。このアクセス権チェックでは、ユーザにパスワードではなく、キーデータを入力させ、それが、PCカード1dから読み出したパスワードから生成したキーデータと比較される。そして、アクセス権を有すると判定された場合には、データ書き込み/読み出し要求に応じてライトデータの暗号化およびその暗号化データの書き込み、または暗号化データの読み出しおよびその復号化を行う。したがって、使用中のPCカード1dに対してもその媒体単位で秘匿性の高い暗号化処理を容易に行うことができる。

【0052】また、記憶媒体には実際にデータ暗号化および復号化の際に使用されるキーデータを格納しておくのではなく、あくまでもそのキーデータを生成するための元となるパスワードのみが格納されているので、第三者が記憶媒体内のデータを単純に解析しただけでは秘匿を解くことはできない。よって、個人単位で携帯され、且つ計算機システムに着脱自在に装着して使用されるという特徴を持つ可搬型記憶媒体のセキュリティ保持に適したアクセス制御を実現できる。

【0053】なお、ユーザに対するPCカードへの秘匿(暗号)化設定についての選択や、パスワードあるいは暗号化/復号化キーデータの入力を促す際のアナウンス手段として、本実施形態では計算機システム本体の表示装置を使用するように述べたが、図示しない計算機システム本体の音声出力装置により行う音声でのアナウンスなどであっても良い。また、表示形態としては、GUIを考慮したものであっても良い。また、データの暗号化および復号化処理として、本実施形態では具体的にその方式について述べなかったが、この方式については秘密鍵暗号方式や公開鍵暗号方式であっても良い。また、アクセス権をチェックする際に、キーデータが一致するまでのリトライ回数を複数回設けても良い。さらに、PCカード内に格納されるパスワードデータについて、本実施形態では、PCカード内のアトリビュートメモリ内に格納するように述べたが、コモンメモリ内であっても良い。暗号化するデータについてもPCカード全体であっても良いし、ディレクトリやファイル単位で行っても良い。

【0054】また、本発明のデータの秘匿(暗号)化設定および秘匿化設定解除によるデータI/O制御方法については、PCカードのみでなく、シリコンディスクやミニディスク、DVDなどの可搬型記憶媒体全てに応用可能な技術である。特に、秘匿化の設定および設定解除



13

を記憶媒体の計算機システム本体への装着時に行うようにすることにより、ユーザに負担をかけることなく行うことができるため、今後、個人情報のセキュリティが強化する傾向にあることから、本発明は有効である。

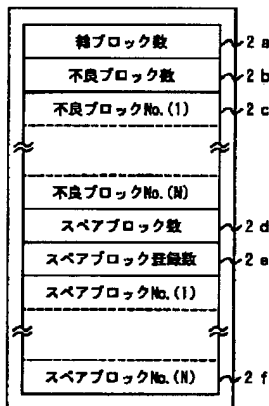
【0055】

【発明の効果】以上説明したように、この発明によれば、PCカードなどの可搬型記憶媒体に既に格納されているデータを暗号化して再格納する処理を具備することにより、使用中の可搬型記憶媒体に対しても暗号化の設定が可能となり、様々な小型携帯機器で使用され、今後益々個人レベルでの使用頻度が増加するPCカードなどの秘匿性を向上させることができる。また、可搬型記憶媒体の計算機システム本体への装着時に暗号化されたカードであるか否かを判別し、暗号化されたカードの場合はアクセス権チェック処理を行うことにより、ディレクトリやファイル単位でなくカード単位でのデータの暗号化を実現し、ユーザの操作に負担をかけることなくすることができる。さらに、暗号化解除処理を新たに追加したことにより、データ処理本体に可搬型記憶媒体を装着し、その記憶媒体に対するアクセス権チェックステップにてアクセス権を取得した時点で、暗号化されたPCカードを通常の状態に戻すことを実現することができる。

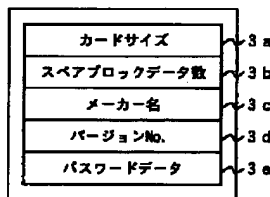
【図面の簡単な説明】

【図1】この発明の一実施形態に係るアクセス制御方法

【図2】



【図3】



14

が適用される計算機システムの構成を示すブロック図。

【図2】同実施形態の計算機システムで使用されるPCカードのデータ管理構造を説明するための図。

【図3】同実施形態の計算機システムで使用されるPCカードのアトリビュートメモリのデータ構造を説明するための図。

【図4】同実施形態の計算機システムにおけるアクセス制御処理の流れを説明するフローチャート。

【図5】同実施形態の計算機システムにおけるPCカード暗号化設定処理の流れを説明するフローチャート。

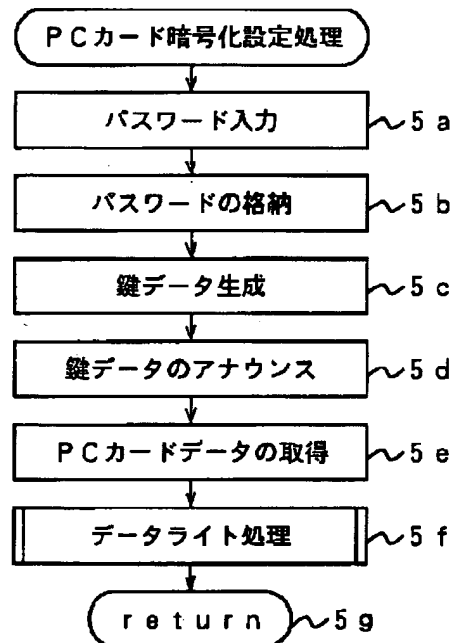
【図6】同実施形態の計算機システムにおけるPCカード暗号化設定解除処理の流れを説明するフローチャート。

【図7】同実施形態の計算機システムにおけるデータI/O処理の流れを説明するフローチャート。

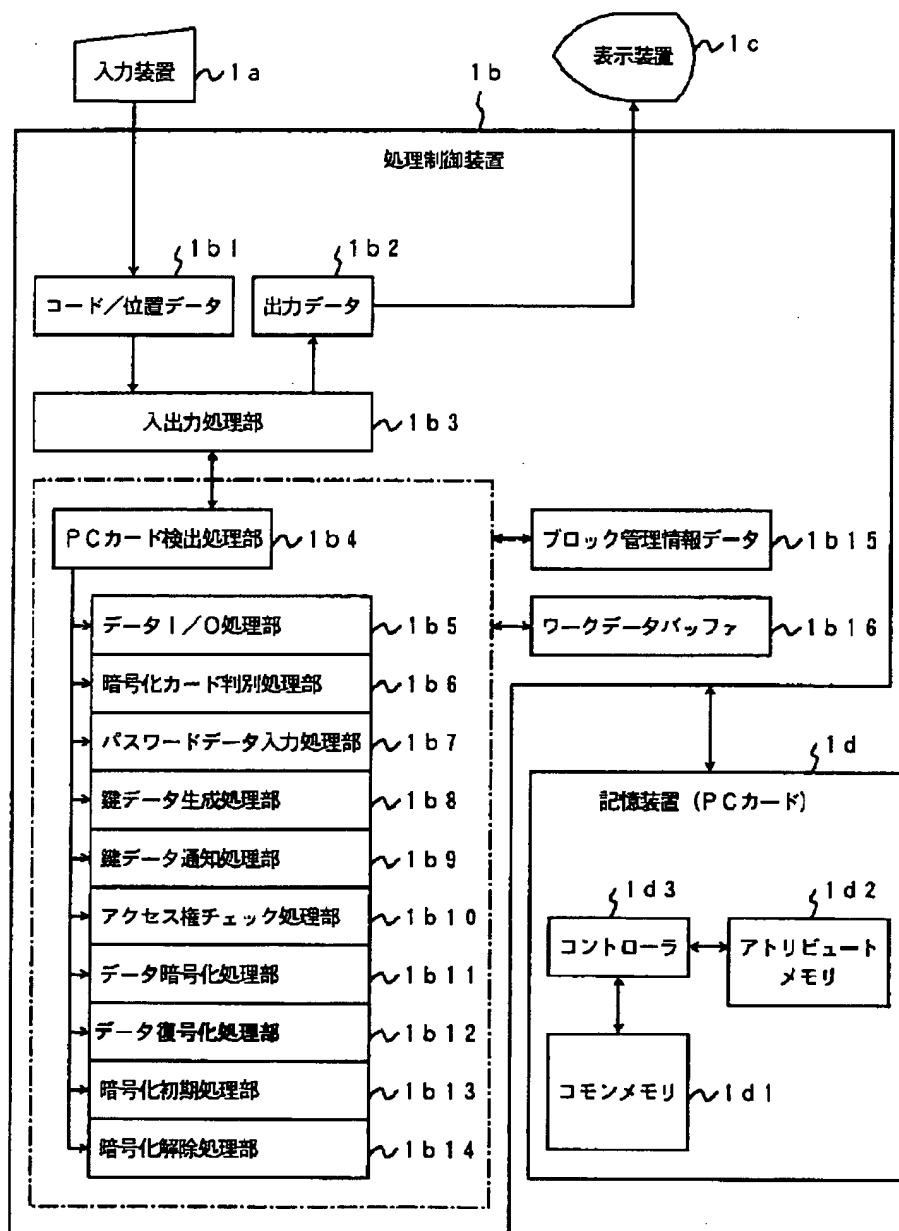
【符号の説明】

1b…処理制御装置、1d…PCカード、1b4…PCカード検出処理部、1b5…データI/O処理部、1b6…暗号化カード判別処理部、1b7…パスワードデータ入力処理部、1b8…鍵データ生成処理部、1b9…鍵データ通知処理部、1b10…アクセス権チェック処理部、1b11…データ暗号化処理部、1b12…データ復号化処理部、1b13…暗号化初期処理部、1b14…暗号化解除処理部。

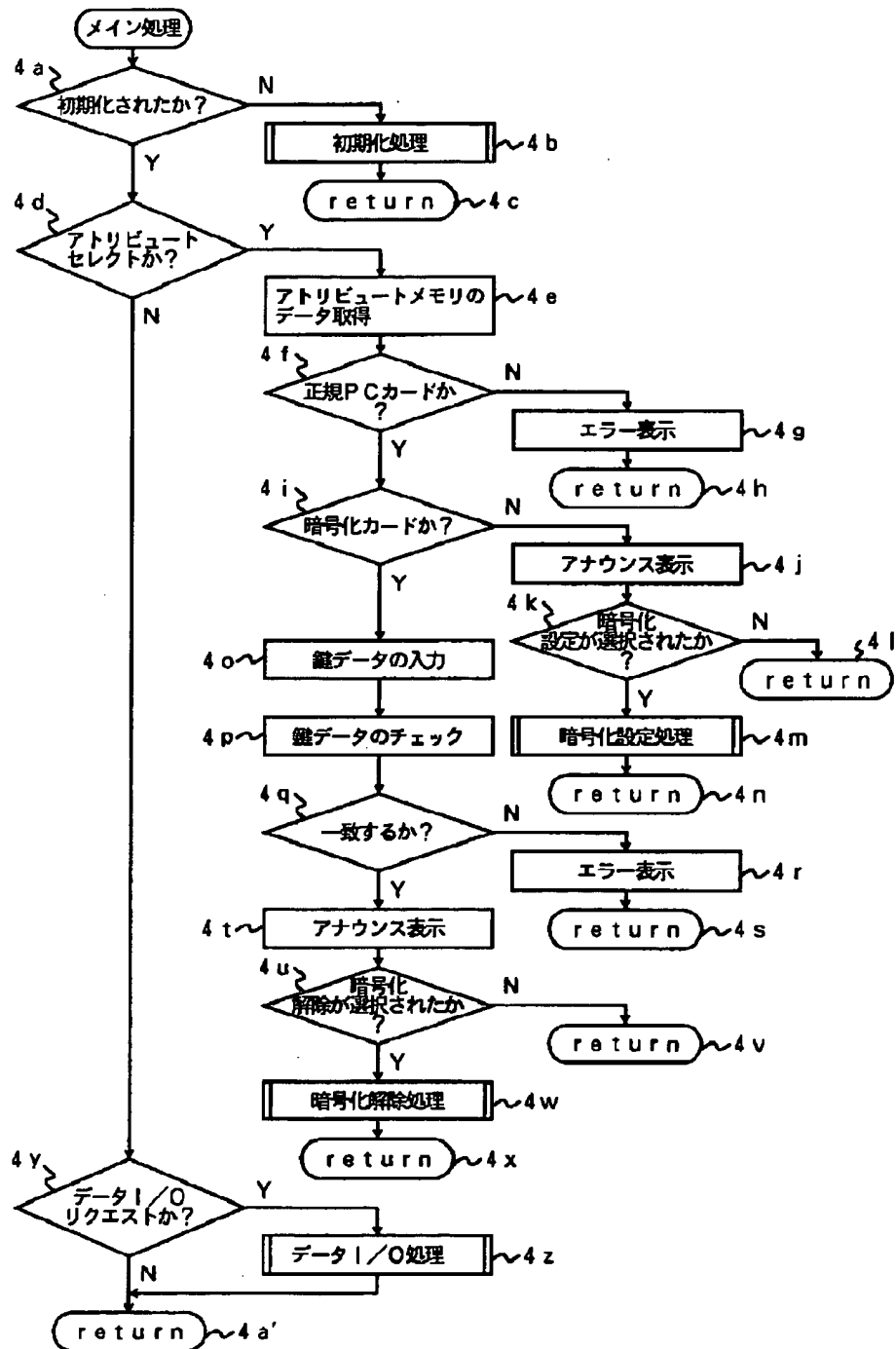
【図5】



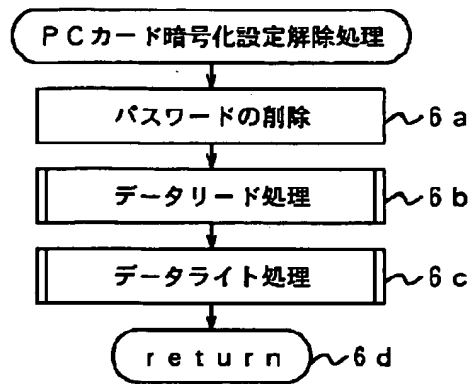
【図1】



【図4】



【図6】



【図7】

